09/936570
JC16 Rec'd PCT/PTO SEP 14 2001

PATENT
2565-0236P

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant: SORIMACHI, Toru et al. Conf.:

Int'l. Appl. No.: PCT/JP00/09129

Appl. No.: NEW Group:

Filed: September 14, 2001 Examiner:

For: ENCRYPTOR, ENCRYPTING METHOD, DECRYPTOR, DECRYPTING METHOD, AND COMPUTER READABLE RECORDING MEDIUM HAVING PROGRAM STORED THEREIN

PRELIMINARY AMENDMENT

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, DC 20231

September 14, 2001

Sir:

The following Preliminary Amendments and Remarks are respectfully submitted in connection with the above-identified application.

AMENDMENTS

IN THE SPECIFICATION:

Please amend the specification as follows:

~~Before~~ line ~~1~~ 5, insert --This application is the national phase under 35 U.S.C. § 371 of PCT International Application No. PCT/JP00/09129 which has an International filing date of December 22, 2000, which designated the United States of America and was not published in English.--

KAM 10/25/02

BEST AVAILABLE COPY

AMENDMENTS TO THE SPECIFICATION

Pages 28-29

KAM 10/25/06

Please replace the paragraph commencing at line ~~15~~ 11 of page 28 with the following amended paragraph:

At the time of T0, the key K_1 is supplied, and the encrypting process of the plaintext data M_1 is started. When the encrypting process of the plaintext data M_1 is started at the time of T0, the input of the selector 54 is switched to B after the initial value ~~IT~~ IV is once input from the input A of the selector 54. Further, at the time of X during the plaintext data M_1 is being encrypted using the key K_1, it is assumed an interrupt IT for requesting to encrypt the plaintext block data N_1 is generated. The ciphertext block data C_1 becomes to be stored in the memory 55 by the time of T1. Then, at the time of T1, the key K_2 is supplied to the encrypting module 51 due to the generation of the interrupt IT. Further, the selector 54 sets the input to A at the time of T1. The switch 57 is connected to F at the time of T1. After the time of T1, the plaintext block data N_1 is encrypted using the key K_2, and the ciphertext block data D_1 is output. At the time of Y, it is assumed the encryption of the plaintext block data N_1 is finished, and the interrupt IT is resolved. Due to the resolution of the interrupt IT, at the time of T2, the key K_1 is supplied to the encrypting module 51, the input of the selector 54 is switched to C, and the switch 57 is connected to E. By switching the selector 54 to C, the ciphertext block data C_1 stored in the memory 55 is input for encrypting the plaintext block data M_2, the plaintext block data M_2 is encrypted by the encrypting module using the key K_1, and the ciphertext block data C_2 is output. Before the time of T3, the input of the selector 54 is switched to B. In case of encrypting the plaintext block data M_3, the ciphertext block data C_2 is fed back from a feedback line 65 of a feedback loop and input, the plaintext block data M_3 is encrypted by the encrypting module using the key K_1, and the ciphertext block data C_3 is output.